خصوصية الجريمة الإلكترونية بين مد الحداثة وجزر التعقيد

The Specificity of Cybercrime between Modernity and Complexity

مخلوف مخلوف *
جامعة مصطفى اسطمبولي-معسكر، الجزائر
m.makhlouf@univ-mascara.dz

خلافي ربيعة
جامعة مصطفى اسطمبولي-معسكر، الجزائر
khelafi.rabia@univ-mascara.dz

- تاريخ الإرسال: 2025/06/26 - تاريخ القبول: 2025/11/22- تاريخ النشر: 27/ 2026/07

الملخص: إن التطور التقني و المعلوماتي الحديث أدى إلى خلق نوع جديد من الجرائم أطلق عليها باسم الجرائم المعلوماتية أو ceber crime كون أنها تقع أو تطال بالمعلومات والمعطيات الرقمية وأنظمة حفظها وطرق تخزينها، والآليات والبرامج المعدة لها كالحاسوب و توابعه و الأنظمة المعلوماتية الخاصة به، هذه الجرائم التي تزايدت حاليا بشكل متصاعد وخطير، وذلك كله في ظل ضعف آليات الحماية وقصورها على توفير الحماية الكافية لها، وتطور صور التعدي بشكل متسارع ولافت، وهو الأمر الذي استدعى ضرورة التدخل التشريعي لمجابهة وصد كل أشكال التعدي الالكتروني، وهو نفس التصور الذي تبناه المشرع الجزائري إذ سعى إلى تعديل قانون العقوبات ليعالج أهم الجرائم الالكترونية التي تطال بالأنظمة الخاصة بالمعالجة الآلية للمعطيات لهدف تأطير هذا النوع من الجرائم ومحاولة التخفيف إن لم نقل الحد منها.

الكلمات المفتاحية: الجرائم المعلوماتية، الحاسب الآلي، الأنترنيت، أنظمة المعالجة الآلية للمعلومات، أشكال الجريمة الالكترونية.

Abstract: Modern technological and information development has led to the creation of a new type of crimes called cybercrimes, as they occur or affect digital information and data, their preservation systems and storage methods, and the mechanisms and programs prepared for them, such as computers, their accessories, and their information systems. These crimes have currently increased in an escalating and dangerous manner, all of this in light of the weakness of protection mechanisms and their failure to provide adequate protection for them. The forms of cybercrime have developed rapidly and significantly, which has necessitated legislative intervention to confront and combat all forms of cybercrime. This is the same vision adopted by the Algerian legislator, who sought to amend the Penal Code to address the most important cybercrimes affecting systems for automated data processing, with the aim of regulating this type of crime and attempting to mitigate, if not limit, it.

Keywords: cybercrime- computer- internet- automated information processing systems- electronic forms of crime.

* المؤلف المرسل: مخلوف مخلوف.

مقدمة:

تميز العصر الحديث بالعديد من الاختراعات و الاكتشافات العلمية الفارهة أهمها ظهور شبكة الانترنيت وانتشارها بقوة عبر العالم، وتطور وسائل تكنولوجيا الاعلام والاتصال وما تحويه هذه الأخيرة من تقنيات ومعدات وبرامج بات استخدامها أمرا هاما وأساسيا في جميع المجالات التي لا تتعلق بحياة الفرد أو الجماعة فقط، بل بمصالح أخرى معتبرة تمس قطاعات عريضة في الدولة تمس بمؤسساتها وهيئاتها في جميع مستوياتها، وعلى ذلك أصبحت المعلوماتية تشهد حضورا قويا ومميزا في جميع المجالات العلمية والبحثية، وبصورة شاملة كل الحياة الاقتصادية و الاجتماعية، ومن جانب آخر مكنت تقنية المعلومات من تطوير أساليب أنظمة المعلومات بهدف الاطلاع على المعلومات وتبادلها ومعالجتها آليا بواسطة الحاسوب و شبكة الانترنيت، حيث مهدت المجال أمام الدول لتطبيق منظومة الحكومة الالكترونية و الاعتماد على التجارة الالكترونية في ظل مفهوم حديث لاقتصاد عالمي رقمي حديث.

غير أنه وبالمقابل صاحب هذا التقدم العلمي والرفاهية في شكلهما الإيجابي ظهور أنماط جديدة من الجرائم يتم بموجبها الاعتداء على هذه الأنظمة والتقنيات المعلوماتية المتقدمة، بحيث انصرف أثرها إلى الغير سواء في شخصه أو في ماله، حيث أصبح الحاسب الآلي والانترنيت على وجه الخصوص وسائل أو محلات لتلك الاعتداءات، لذا أطلق عليها تسمية الجرائم الالكترونية أو المعلوماتية وحتى السيبرانية[1] في بعض المؤلفات أو المواقع.

ومن بين أشكال هذه الجرائم نجد على وجه الخصوص الجرائم الماسة بالأنظمة الآلية للمعطيات، أي الجرائم التي يكون النظام المعلوماتي محلا لها، ومثال ذلك في جريمتي الدخول والبقاء داخل منظومة للمعالجة الآلية للمعطيات، وجريمتي التعدي على المعطيات والتعامل في معطيات غير مشروعة.

وأمام هذا النشاط الاجرامي غير المسبوق سعت العديد من الأنظمة القانونية في شتى دول العالم إلى محاولة التصدي لكبح هذا النوع من الجرائم بالنظر لجملة آثارها غير المشروعة أو غير المرغوب فيها، سواء على الأشخاص أو الأموال وحتى المؤسسات.

[1] –عباس كريمة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مجلة البيبان للدراسات القانونية والسياسية، العدد الرابع، ديسمبر 2017، ص119.

ومن هذا المنطلق تبرز الإشكالية الرئيسية التي سنحاول الإجابة عنها في هذه الدراسة والمتمثلة فيما المقصود بالجرائم الالكترونية؟ وماهي المجالات التي تطال بها؟

هذا ويتمحور الهدف الأساسي من هذه الدراسة في محاولة الاجابة عن مضمون الاشكالية المتقدمة، وذلك بداية بالتعرض للإطار النظري أو المفاهيمي للجرائم الالكترونية عموما قصد التعرف على ملامحها وبيان صورها، بالإضافة إلى محاولة استعراض أهم العناصر المكونة لها وبيان أشكالها ومن ثمة التعرض لكيفيات ارتكابها داخل البيئات الرقمية.

ومن أجل تغطية هذا الهدف المتقدم اعتمدنا على المنهج الوصفي خاصة عند محاولتنا لضبط مفهوم دقيق للظاهرة واستعراض أهم صورها والكيفيات المنتهجة في ارتكابها.

وللإحاطة الشاملة بكافة جوانب الموضوع قسمنا هذه الدراسة إلى محورين رئيسيين، أما الأول منهما فورد تحت مسمى **نطاق الجريمة الإلكترونية**، في حين يرد الثاني منهما بعنوان **أشكال ارتكاب الجرائم الإلكترونية**.

1- نطاق الجريمة الإلكترونية.

بداية تجدر الإشارة إلى أنه لم يتفق الفقه الجنائي بعد على وضع تعريف موحد لهذا الصنف من الجرائم، كما أنه لم يتفق أيضا على وضع تسمية موحدة تشير إليها، فمنهم من أطلق عليها وصف الجريمة الالكترونية وآخر بالجريمة المعلوماتية، في حين ذهب البعض إلى تسميتها بجرائم الحاسب الآلي أو الجريمة الرقمية على أساس لغة الحاسب الآلي[2]، وحتى جرائم إساءة استعمال أو استخدام تكنولوجيا الإعلام والاتصال، بالإضافة إلى تسميتها بالجرائم الناعمة كون أنه ينعدم فيها العنف المادي ضد الضحية أثناء تنفيذها بعكس ما هو عليه الحال في الجرائم التقليدية.

وتجدر الإشارة إلى أن هناك اختلاف من حيث ميدان ارتكاب الجريمة الالكترونية أو المعلوماتية الذي يمكن تقسيمه إلى جرائم الحاسب الآلي وميدان جرائم شبكة الانترنيت، فبينما تتحقق الأولى منهما بالمساس أو التعدي على مكونات الحاسب الآلي وبرامجه والمعلومات المخزنة به، فإن الثانية تتحقق بالنقل الغير مرخص به للمعلومات والبيانات بين أجهزة الكمبيوتر عبر الشبكات الرقمية، غير أن الواقع التقني

[2] –مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، دار النهضة العربية، مصر، 2008، ص112.

الحالي أدى إلى اندماج ميادين الحوسبة والاتصالات. ومن ثمة ظهور مصطلح عام يجمع بين شكلي الجريمتين السابقتين يطلق عليه بCybercrime، وانقسم على إثر ذلك رأي الفقه الجنائي في تحديد مفهوم للجريمة ومنه تحديد نطاقها الموضوعي بين من ينظر إليها بمنظور ضيق وآخر بالموسع وفيما يلي استعراض لأهم هذه الآراء.

1.1- تحديد نطاق الجريمة الالكترونية من خلال مفهومها الضيق.

يرى رواد هذا الاتجاه ضرورة التضييق في مفهوم هذه الجريمة إذ عرّفها جانب من هذا الفقه وعلى رأسهم الفقيه الألماني Tiedmann بأنها كل جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات[3]، كما عرفها أيضا ذات الفقيه على أنها كل جريمة تقع ضد المال مرتبطة بالمعالجة الآلية للمعلومات عن طريق نسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر، أو تلك التي يتم تحويلها عن طريقه[4].

في حين عرفها الفقيه الفرنسي Masse بأنها الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح[5]، وعبر عنها آخرون بأنها جرائم الأموال وجرائم الأشخاص وجرائم المصلحة العامة التي تقع عن طريق استعمال الانترنيت سواء داخل البلاد أو خارجها[6].

ومن جملة هذه التعريفات الفقهية نجد أيضا تعريف الأستاذ Tom Forester والأستاذ Eslie D. Ball بأنها فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية[7].

كما تعرّف الجريمة الالكترونية من ذات الزاوية أو الركن بأنها كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر لازم لارتكابه من ناحية، وملاحقته والتحقيق فيه من ناحية أخرى،[8] فحسب هذا التعريف والتعريفات المتقدمة الخاصة بالجريمة الالكترونية فإنه يجب أن تتوافر لدى الجناة في

---

[3] – نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص48.

[4] –أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ص94.

[5] – محمد سامي الشواء، ثروة المعلومات وانعكاساتها على قانون العقوبات، مطابع الهيئة المصرية العامة للكتاب، مصر، 2003، ص19.

[6] –غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنيت، دار الفكر القانوني، مصر، 2010، ص11.

[7] –حاتم أحمد محمد بطيخ، تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات، دراسة تحليلية مقارنة، دون طبعة، دون دار نشر، مصر، دون سنة نشر، ص14.

[8] – نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية، الطبعة الأولى، دار النهضة العربية، القاهرة مصر، 2004، ص21.

– أحمد هلالي عبد اللاه، الجوانب الموضوعية الإجرائية لجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003، ص13.

هذا النوع من الجرائم المعرفة اللازمة والكافية بقدر كبير لتقنيات الحاسبات الآلية، وذلك ليس فقط بالنسبة لهم بل كذلك للأشخاص المكلفين بملاحقة هذا النوع من الجرائم والتحقيق والتحري والبحث عنها.

كما تعرّف الجريمة الالكترونية تبعا لنفس التصور المتقدم بأنها كل جريمة ترتكب داخل محيط أجهزة الحاسوب أو كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها، أو هي تلك الجرائم التي يكون فيها الحاسوب وسيلة لارتكاب فعل غير مشروع أو محل وقوع الفعل غير المشروع، وذلك بالقيام بعمل أو الامتناع عن أدائه من شأنه الاعتداء على الأموال المادية أو المعنوية شريطة أن يكون مرتكبها على معرفة بتقنية استخدام الحاسوب والتعامل مع معطياته[9].

نلاحظ من خلال هذه التعريفات المتقدمة أنها وردت قاصرة في الإحاطة بكافة ملامح أو أوجه ظاهرة الإجرام الالكتروني، فمن الفقه المتقدم ما ارتكز إلى حد كبير في محاولة وضعه تعريف للجريمة الالكترونية على الوسيلة المستعملة في إحداثها التي هي عموما الحاسوب أو الكمبيوتر، كما أنها تضيق إلى حد كبير من نطاق الجريمة الالكترونية، فهي تخرج من مجالها الكثير من الأفعال الغير مشروعة التي يستخدم الحاسوب لارتكابها، وعلى إثر ذلك سعى جانب آخر من الفقه إلى محاولة تغطية هذا النقص من خلال المساهمة في وضع تعريف موسع للظاهرة يشمل جميع الأفعال الغير المشروعة التي تمس بتكنولوجيات الإعلام والاتصال، وذلك على النحو الآتي.

2.1- تحديد نطاق الجريمة الالكترونية من خلال مفهومها الموسع.

على عكس فكر الاتجاه السابق يرى رواد هذا الاتجاه ضرورة التوسع في مفهوم هذه الجريمة، إذ عرفها جانب من هذا الفقه بأنها كل نشاط إجرامي تستخدم فيه – التقنية الالكترونية– الحاسوب الآلي– وشبكة الانترنيت– بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف، بحيث عرفها الفقيهين الفرنسيين Vivant وLe stant بأنها مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب.[10]

[9] – مخلد إبراهيم الزعبي، فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الالكترونية– دراسة مقارنة–، المجلة العربية للنشر العلمي، العدد 37، بتاريخ 2 تشرين الثاني، 2021، ص279.

[10] – نهلا عبد القادر المومني، المرجع السابق، ص49.

وهو نفس المفهوم الذي أكده كل من الفقيهين Michel et Credo على أن الجريمة الالكترونية إنما المقصود بها كل الأفعال الغير مشروعة التي يستخدم فيها الحاسب كأداة لتنفيذها، هذا بالإضافة إلى الحالات المتعلقة بالولوج غير مصرح به لجانب المجني عليه وبياناته، وتمتد هذه الجريمة لتشمل كافة الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحاسب الآلي بما تتضمنه من شيكات تحويل الحاسبات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وحتى سرقة الحاسب في حد ذاته أو مكوناته.[11]

وفي ذات السياق عرفها مختصون ضمن مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين،[12] الذين أشاروا إلى أنها تلك الجريمة التي يمكن ارتكابها بواسطة حاسوب أو شبكة حاسوبية أو داخل نظام حاسوب، في حين عرفتها الاتفاقية الأوروبية للجرائم السيبرانية اتفاقية بودابست[13] بأنها كل النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية.

كما عرفتها أيضا الإجابة البلجيكية على الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية O.E.C.D عام 1983 حول الغش المعلوماتي، بأنها كل فعل أو امتناع عن فعل من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.

غير أن ما يؤخذ على هذا الفقه هو الآخر أنه قد بالغ في توسيع نطاق الجريمة الالكترونية أو المعلوماتية، إذ يعاب عليه أنه قد أسقط وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك على اعتبار أنه قد استعمل الحاسوب الآلي في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا لا يمكن إعطائها وصف الجريمة الالكترونية[14].

---

[11] –أحمد هلالي عبد اللاه، المرجع السابق، ص14، وفي ذات السياق أنظر: طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة مقدمة لنيل شهادة الماجستير في القانون الجنائي، كلية الحقوق والعلوم السياسية بجامعة الجزائر 01، 2011–2012، ص06.

[12] – مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا خلال فترة ما بين 10 إلى 17 ابريل 2000.

[13] – انعقدت الاتفاقية الأوروبية لجرائم الانترنيت اتفاقية بودابست في عاصمة المجر بودابست بتاريخ 2001/11/23 بمصادقة 26 دولة من الدول الأعضاء في مجلس أوروبا البالغ عددها 48 دولة بالإضافة إلى دول غير أعضاء في مجلس أوروبا وهي الو.م.ا واليابان وكندا وجنوب إفريقيا وذلك وفقا لنص المادة 38 من الاتفاقية التي تجيز انضمام الدول غير الأعضاء في مجلس أوروبا وفي آخر إحصائية بتاريخ 2014/10/05 وقعت على الاتفاقية 45 دولة من الدول الأعضاء من أصل 47 دولة وبقيت دولتان لم توقعا هما روسيا وسان مارينوا. انظر: الجريمة الالكترونية وكيفية مواجهتها من إعداد: مجمع البحوث والدراسات أكاديمية السلطان قابوس لعلوم الشرطة نزوى، سلطنة عمان، 2016، ص11.

[14] – ونوغي نبيل وزيوش عبد الرؤوف، الجريمة الالكترونية في التشريع الجزائي، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الجلفة، المجلد الرابع، العدد 03، الجزائر، 2009/09/01، ص131.

وأمام هذا الجدل الفقهي القائم حول مسألة وضع مفهوم محدد و دقيق للجريمة الالكترونية بين من يوسع من نطاق مفهومها ومن يضيق منه، وجب علينا الاهتداء لموقف المشرع الوطني من هذا الشأن، وكيف ساهم هذا الأخير في محاولة ضبط مفهوم لهذه الظاهرة الإجرامية المستحدثة من خلال جملة القوانين المتعلقة بها، وهذا ما يمكن استنباطه من نص المادة 02 الفقرة 1 من القانون 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[15] **على أنها: " تلك الجرائم الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.**"[16]، كما نص على سلسلة من الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات بموجب المواد من 394 مكرر إلى 394 مكرر 7 من القانون 04-15 المعدل والمتمم لقانون العقوبات الجزائري[17].

وبالتمعن في نصوص هذه المواد نستنتج أن المشرع الجزائري قد قسم هذه الجرائم المستحدثة إلى ثلاثة أنواع أهمها:

- جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية.
- جرائم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الالكترونية.

2- أشكال وصور ارتكاب الجرائم الإلكترونية.

تعد عملية تصنيف الجرائم الالكترونية عملية أشد تعقيدا من تلك المتعلقة بتصنيف الجرائم التقليدية، وذلك راجع إلى كون أن هذه الجرائم تقع أولا في فضاء افتراضي لا مادي، بالإضافة إلى أنها تشمل وتستهدف العديد من القطاعات من أشخاص طبيعية كانت أم معنوية وحتى الدول، وذلك من خلال إمكانية مساسها بأمنها واستقراها اجتماعيا وسياسيا وحتى اقتصاديا، والأمر كذلك عائد إلى تشعبها واتساع مجالها، إضافة إلى سرعة تطورها.

---

[15] – القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها جريدة رسمية رقم 47 المؤرخة 16-08-2009 من صفحة 05 إلى 09.

[16] –وهو التعريف المستمد من الاتفاقية الدولية حول الجرائم المعلوماتية اتفاقية بودابست السالفة الذكر.

[17] – القانون 04-15 الصادر في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 الصادر في 18 جوان 1966 المتضمن قانون العقوبات جريدة رسمية العدد 71.

لذلك لم يستقر الفقه القانوني على تصنيف موحد لها، فمن الفقه من صنفها بالنظر إلى مرتكبيها، وهناك ما قام بتصنيفها تبعا لطريقة تنفيذها، وأخرى تبعا للغرض أو الهدف من الاعتداء[18] الكامن ورائها، بالإضافة إلى محاولة تصنيفها وفق معيار محل الجريمة أو الضحايا وهو المعيار الذي سنتبناه في تقسيمنا لأصناف الجريمة الالكترونية عبر تقسيمها إلى جرائم واقعة على الأشخاص وأخرى على الأموال، وقسم أخير يضم الجرائم الواقعة على الدولة، وذلك على النحو الآتي:

1.2- الجرائم الالكترونية الواقعة على الأشخاص.

وهي الجرائم الالكترونية التي يكون ضحاياها أشخاص طبيعيين، ويمكن حصرها في الجرائم الماسة بحقوق الملكية الفكرية، والجرائم التي تمثل اعتداء على الحياة الخاصة للأشخاص، وجرائم انتحال الشخصية.

1.1.2- الجرائم الالكترونية الواقعة على حقوق الملكية الفكرية.

يكون النظام المعلوماتي الأداة المباشرة للاعتداء على حقوق الملكية الفكرية بنوعيها الأدبية الفنية والصناعية التجارية و ما تشمله من مفردات، وتكون صورتها في الاستيلاء على المجهود الفكري وإبداع المؤلفين، ومثال ذلك السطو على بنك المعلومات المتمثل في مجموع البيانات المخزنة في شكل أعمال أو مجهودات فكرية خالصة المخزنة في نظام المعالجة الآلية، وتخزين أو استخدام هذه المعلومات دون ترخيص أو إذن من صاحبها (كون أن هذه الأعمال تعتبر حقوق معنوية ذات قيمة أدبية ومالية معتبرة يستلزم التصرف فيها إذن صاحبها)، وكذلك نسخ وتقليد البرامج و إعادة إنتاجها و صنعها دون ترخيص[19]. وتكون محلا لهذه الاعتداءات براءات الاختراع والرسوم والنماذج الصناعية، والعلامات التجارية والأسماء التجارية وحقوق الملكية الأدبية والفنية – حقوق المؤلف والحقوق المجاورة- المحمية بموجب قوانين خاصة[20].

[18] – عبد السلام محمد المايل، عادل محمد الشريجي، على قابوسة، الجريمة الالكترونية في الفضاء الالكتروني- المفهوم الأسباب سبل المكافحة مع التعرض لحالة ليبيا، مجلة أفاق البحوث والدراسات- سداسية دولية محكمة-، المركز الجامعي ايليزي، العدد 04 جوان 2019، ص250.

[19] – غانم مرضي الشمري، الجرائم المعلوماتية، الدار العلمية الدولية، الطبعة الأولى، عمان،2016، ص52.

[20] – الأمر رقم 07/03 المؤرخ في 2003/07/19 المتعلق ببراءة الاختراع الجريدة الرسمية العدد44 لسنة 2003 والأمر رقم 05/03 المؤرخ في 2003/07/19 المتعلق بحقوق المؤلف والحقوق المجاورة، الجريدة الرسمية، العدد 44 لسنة 2003.

2.1.2- الجرائم الالكترونية الواقعة على حرمة الحياة الخاصة.

كرس الدستور الجزائري حرمة الحياة الخاصة للمواطن وحرص على حمايتها من كل أشكال التعدي، ولما كان الحاسب الآلي الأداة المستحدثة لتخزين أهم المعلومات والبيانات الشخصية المتعلقة بالأشخاص، وذلك لقدرته على تخزين أكبر عدد من المعلومات، هذا ما جعل له الدور المحوري في إمكانية الإفشاء عنها إذا ما تم اختراقه.

ومثال ذلك ما يقوم به بعض الهاكرز أو قراصنة الحواسيب الآلية من أعمال تمس خصوصية الضحايا في أبدانهم أو شرفهم، إذ يسعى المجرمون في هذا الصدد إلى محاولة بعث الرهبة والخوف في نفسية الضحية ببعث رسائل مجهولة المصدر عن طريق البريد الالكتروني فتخاف الضحية من الفضيحة[21]، ما يدفعها إلى الدخول في مفاوضات مع الجاني قصد التكتم عن هذه الأسرار وعدم الإفشاء بها للعلن مقابل أداءات مالية تدفع للجاني أو ما يقوم مقام ذلك من مكاسب غير مشروعة. وتتم هذه الأعمال عادة عن طريق اعتراض المكالمات الصوتية أو الصوتية المرئية للضحية، ومحادثاتها أو رسائلها في شكله المكتوب أو المسموع، أو بإعداد ملف يحتوي على معلومات خاصة بشخص دون علمه.

3.1.2- الجرائم الالكترونية المرتبطة بانتحال شخصية.

بسبب التنامي المتزايد لشبكة الانترنيت الذي أعطى للمجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة والاستفادة منها في ارتكاب جرائمهم، أصبحت تنتشر عبر شبكة الانترنيت الكثير من الإعلانات المشبوهة والتي تحاكي العمل الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية[22]، وتطال هذه الجريمة الأشخاص وحتى المواقع.

حيث يستولي المجرم الالكتروني على البيانات والمعلومات الشخصية المتعلقة بالضحية بعد اختراق موقعه بسبب إما سمعته أو مكانته الاجتماعية أو وظيفته من أجل الاستفادة الغير مشروعة من الصلاحيات التي تمنحها له هذه الأخيرة بغية الاستفادة منها ماديا ومعنويا بوجه غير مشروع.

---

[21] –بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، المجلد 14، العدد04، 2021، ص56.

[22] –روان بنت عطية الله الصحفي، الجرائم السيبرانية، المجلة الالكترونية الشاملة متعددة التخصصات، العدد 24، شهر ماي 2020، المملكة العربية السعودية، ص18.

4.1.2- الجرائم الالكترونية الماسة بجانب الأخلاق.

وتشمل تحريض القاصرين على أنشطة جنسية غير مشروعة وإفسادهم بأنشطة جنسية عبر الوسائل الالكترونية، و إغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة وتلقي أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة، والتحرش الجنسي بالقاصرين عبر الكمبيوتر والوسائل التقنية و نشر و تسهيل نشر و استضافة المواد الفاحشة عبر الانترنيت بوجه عام و للقاصرين بوجه خاص، و نشر الفحش و المساس بالحياء واستخدام الانترنيت لترويج الدعارة بصورة قسرية، والحصول على الصور والهويات بطريقة غير مشروعة لاستغلالها في أنشطة غير مشروعة. وهي أوصاف تجتمع كلها تحت صورة واحدة وهي استغلال الانترنيت و الكمبيوتر لترويج الدعارة وإثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة[23].

5.1.2- الجرائم الالكترونية المتعلقة بالسب والقذف.

هي أكثر الجرائم انتشارا على شبكة الانترنيت عن طريق وسائل الاتصال بالكتابة أو البريد الالكتروني أو غرف المحادثة، وذلك بتوجيه وإسناد واقعة أو خدش شرف الأشخاص أو دون إسناد واقعة، والهدف من كل ذلك هو تشويه السمعة، ومثالها في جرائم سب الرسول صلى الله عليه وسلم أو رئيس الجمهورية [24].

2.2- الجرائم الالكترونية الواقعة على الأموال.

بالإضافة إلى الجرائم المتقدمة التي تمس أو تطال بالأشخاص هناك صنف أخر من الجرائم يقع على الأموال، والتي قد تتخذ الصور التالية:

1.2.2 - جريمة السرقة الواقعة على البنوك: والمقصود هنا ليس السرقة بمفهومها التقليدي وإنما سرقة البنوك بطرق الكترونية أو معلوماتية، وذلك عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم من زبائن وعملاء والتخفي وراء شخصيتهم، ما يدفع بالبنك إلى تحويل الأموال الكترونيا أو ماديا إلى حسابات أخرى تعود للجاني.

---

[23] -يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، قانون العقوبات، قانون الإجراءات الجزائية، قوانين خاصة، دار الجامعة الجديدة، 2019، ص44.

[24] -غانم مرضى الشمري، المرجع السابق، ص56.

وتتمثل عمليات السرقة الالكترونية أيضا في الاستيلاء على ماكينات الصرف الآلي و البنوك، بحيث يتم فيها نسخ البيانات الالكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية، أو إنشاء صفحة انترنيت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل إدخال بياناته أو تحديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها[25].

2.2.2- جريمة غسيل الأموال.

تمارس هذه الجريمة عبر الانترنيت، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم القذرة بتوفير السرعة وتفادي الحدود الجغرافية والقوانين المعيقة لغسيل الأموال، وكذا تشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصبغة الشرعية[26].

3.2.2- جريمة تزوير المستندات والتوقيعات الالكترونية.

يقصد عموما بالتزوير تغيير الحقيقة في محرر يمكن أن يستخدم في إثبات حق أو واقعة يترتب عليها نتائج قانونية غشا و إضرارا بالغير بواسطة إحدى الوسائل المحددة قانونا،[27] ولاشك أن الاعتماد الحالي منقطع النظير على الحاسبات الآلية كونها الأداة المثالية لتخزين المعلومات الهامة التي تحويها المستندات الالكترونية كالبيانات المتعلقة بشهادات الميلاد و الوفاة وجوازات السفر ورخص القيادة وغيرها من ملفات هامة، كان ذلك دافعا للتعدي على هذه المستندات الرسمية من طرف البعض، إذ يتم تزويرها عبر وسائل جد متطورة أهمها الماسح الضوئي لإحداث وثائق مطابقة للأصل لكنها في حقيقة الأمر مزيفة أو مقلدة، وحتى تزوير التوقيعات الالكترونية.

---

[25] -يزيد بوحليط، المرجع السابق، ص45.

[26] – سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، مجلة الدراسات الإعلامية، المركز الديمقراطي العربي، العدد الأول، يناير 2018، ص244.

[27] – اللجنة العلمية لمعهد الكويت للدراسات القضائية والقانونية، الجرائم الالكترونية، دون طبعة، معهد الكويت للدراسات القضائية والقانونية، الكويت 2018-2019، ص21.

3.2- الجرائم الالكترونية الواقعة على الدولة.

إلى جانب الجرائم الالكترونية الواقعة على الأشخاص الطبيعية والأموال نجد أن هناك مجموعة من الجرائم الالكترونية تقع على الدولة كشخص اعتباري عام، وتتمثل هذه الجرائم أساسا في جريمتي المساس بأمن الدولة وكذلك الإرهاب الالكتروني.

1.3.2- جريمة المساس بأمن الدولة.

استغلت الكثير من الجماعات المتطرفة الصبغة الاتصالية للأنترنيت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة اللذان أخذا معنى آخر في استعمال الانترنيت التي سمحت لهم في ارتكاب جرائم في غاية الشنع بحق المجتمعات والدول[28]على حد سواء.

ومن نماذج هذه الجريمة الاطلاع الغير مرخص به على مختلف الأسرار العسكرية الاقتصادية للدول، ونشر الفتنة وخطابات الكراهية في أوساط المجتمع قصد خلق فوضى وإحداث صراعات وانشقاقات داخلية فيها.

2.3.2- جريمة الإرهاب الالكتروني.

يتم في هذه الصورة بث ثقافة الإرهاب عبر الانترنيت عن طريق تأسيس مواقع افتراضية تتمثل في المنظمات، وهي مواقع شهدت تزايدا مستمرا في السنين الأخيرة توازيا مع زيادة المنظمات الإرهابية والفكر التطرفي، حيث تعلن عبر هذه المواقع تحملها مسؤولية إحدى الهجمات التي ارتكبت، أو بيانات تنفي أو تعلق على الأخبار الصادرة عن المنظمات أو جهات دولية أخرى[29] حول أحداث إرهابية مرتكبة.

[28] – بوضياف أسمهان، المرجع السابق، ص358.

[29] – سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة لنيل شهادة ماجستير، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة 2014، ص34.

الخاتمة:

توصلنا من خلال ما سبق التعرض له في موضوع دراستنا المتعلق بخصوصية الجرائم الالكترونية و بين مد الحداثة وجزر التعقيد و خاصة منها تلك الماسة بأنظمة المعالجة الآلية للمعطيات أنه وفي إطار بحثنا عن مفهوم خاص لهذا النوع من الجرائم لم يتفق الفقه القانوني على تحديد أو وضع تعريف موحد ودقيق لها، وذلك ما قادنا لاستعراض غالب ما جاء به الفقه في هذا الموضوع من تعريفات، و التي وردت إما في مفهومها الضيق أو الموسع، غير أن ما يهمنا من ذلك هو تعريف المشرع الجزائري لها، و الذي يقتبس من مضمون نص المادة 02 فقرة01 من القانون 09/04 : **حين وصفها بأنها تلك الجرائم الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.**

ومن جملة النتائج المتوصل إليها في هذه الدراسة هو محاولتنا لإيجاد مصطلح موحد يعبر عن الظاهرة والتي اتخذ لها جمهور الفقهاء مصطلحا للدلالة أو التعبير عنها كل حسب وجهته.

بالإضافة الى محاولتنا الجادة لإيجاد مفهوم أو تعريف خاص بالجريمة وذلك في ظل تعدد التعاريف القائلة بها بين من تضيق من مفهومها وممن توسع من ذلك.

كما حاولنا وبالموازاة لما تقدم تحديد نطاق الجريمة الالكترونية وبيان خصائصها المميزة عن كل أطياف الجريمة الأخرى سواء الواردة منها في قانون العقوبات العام أو التشريعات الخاصة المرتبطة به.

وعلاوة على ما سبق ذكره سعينا أيضا إلى استعراض أهم صور الجريمة الالكترونية والتي تشهد هي الأخرى اختلاف من حيث تصنيفها، ونحن وبصدد تصنيفنا لهذا النوع من الجرائم اعتمدنا على التصنيف القائم على محل الجريمة وضحاياها، إذ قسمناها إلى جرائم تقع على الأشخاص وأخرى على الأموال وصنف ثالث يضم الجرائم الواقعة على الدولة وأمنها.

ومن جملة ما يمكن أن نوصي به:

-هو ضرورة تعديل وتحيين المنظومة القانونية الجزائرية المتعلقة بالتجريم الالكتروني كي تتكيف والواقع الاجرامي الذي يشهد تطور متزايد.

–ضرورة مراجعة النصوص القانونية المعالجة لموضوع الجرائم الالكترونية في التشريع الجزائري، وذلك بتشديد الوصف الجنائي لها والعقوبات المقررة لها بغية تحقيق الردع الكافي لمواجهته.

–ضرورة تكثيف الجهود الدولية والاقليمية لمحاربة الجريمة الالكترونية بشتى صورها وأثارها، وذلك من خلال إبرام معاهدات واتفاقيات تحد من انتشار هذه الجرائم، ووضع هياكل ومؤسسات ومراكز اقليمية تكافح الجرائم الالكترونية سواء على المستوى العربي أو الافريقي.

–إعداد دورات تدريبية في مراكز متخصصة لرجال المتابعة والتحقيق في الجرائم الالكترونية قصد تمكينهم من المعرفة الشاملة واللازمة لكيفيات التعامل من الأنظمة الآلية لمعالجة المعطيات، وذلك لأجل تسهيل عليهم مهام التحقيق وجمع الدليل في الجرائم الالكترونية، لأن التحقيق في هذه الجرائم يتطلب مهارات فنية عالية.

–التوعية والارشاد والتنديد بخطورة الجرائم الالكترونية، وذلك من خلال تنظيم حملات تحسيسية على مستوى مراكز الاشعاع الثقافي وخاصة الجامعات والمؤسسات التعليمية، وذلك بعقد ملتقيات ومؤتمرات وأيام دراسية تحسيسية بمخاطر الجرائم الالكترونية.